P/4043-23

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Fernando DE LA PUENTE ARRANTE et al. Date: May 21, 2002

Serial No.: 10/069,466 Group Art Unit: --

International Appln. No.: PCT/ES01/00250 Examiner: --

International Filing Date: June 22, 2001

For: EXTERNAL SIGNATURE DEVICE FOR A PC WITH OPTICAL DATA INPUT VIA THE MONITOR

U.S. Patent and Trademark Office
P.O. Box 2327
Arlington, Virginia 22202

SECOND PRELIMINARY AMENDMENT

Preliminary to examination, and further to the Preliminary Amendment filed February 20, 2002, please further amend the above-identified patent application as follows:

FEE CALCULATION

Any additional fee required has been calculated as follows:

_____ If checked, "Small Entity" status is claimed.

	NO. CLAIMS AFTER AMENDMENT		HIGHEST NO. PREVIOUSLY PAID FOR		EXTRA PRESENT		RATE	ADDIT. FEE
TOTAL	13	MINUS	20	* =	0	X	($9 SE or $18)	$ -0-
INDEP.	1	MINUS	3	** =	0	X	($42 SE or $84)	$ -0-
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM						X	($140 SE or $280)	$ -0-
* not less than 20 ** not less than 3							TOTAL	$ -0-

If any additional payment is required, a check which includes the calculated fee of $____ (OFGS Check No. _____) is attached.

In the event the actual fee is greater than the payment submitted or is inadvertently not enclosed or if any additional fee during the prosecution of this application is not paid, the Patent Office is authorized to charge the underpayment to Deposit Account No. 15-0700.

CONTINGENT EXTENSION REQUEST

If this communication is filed after the shortened statutory time period had elapsed and no separate Petition is enclosed, the Commissioner of Patents and Trademarks is petitioned, under 37 C.F.R. § 1.136(a), to extend the time for filing a response to the outstanding Office Action by the number of months which will avoid abandonment under 37 C.F.R. § 1.135. The fee under 37 C.F.R. § 1.17 should be charged to our Deposit Account No. 15-0700.

AMENDMENTS

_✔_ If checked, amendments to the specification and/or claims are submitted herewith.

Specification:

Please delete the paragraph/section beginning at page 3, line 28 to page 3, line 32 and replace such paragraph/section pursuant to 37 C.F.R. § 1.121(b)(ii) with the "clean" version attached hereto as Appendix A. Entry is respectfully requested. A version with markings to show the changes made pursuant to 37 C.F.R. § 1.121(b)(iii) is attached hereto as Appendix B.

3. Claims:

Please amend claims 1-5 and add new claims 7-19 pursuant to 37 C.F.R. § 1.121(c)(i) as set forth in the "clean" version attached hereto as Appendix A. Entry is respectfully requested. A version with markings to show the changes made pursuant to 37 C.F.R. § 1.121(c)(ii) is attached hereto as Appendix B.

REMARKS/ARGUMENT

Claims 1-5 have been amended and claims claims 7-19 have been added to better conform with U.S. practice.

EXPRESS MAIL CERTIFICATE

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail to Addressee (mail label #EL611016688US) in an envelope addressed to: U.S. Patent and Trademark Office, P.O. Box 2327, Arlington, VA 22202, on May 21, 2002:

Dorothy Jenkins
Name of Person Mailing Correspondence

Dorothy Jenkins
Signature

May 21, 2002
Date of Signature

JAF:JJF:ck:sds

Respectfully submitted,

James A. Finder
Registration No.: 30,173
OSTROLENK, FABER, GERB & SOFFEN, LLP
1180 Avenue of the Americas
New York, New York 10036-8403
Telephone: (212) 382-0700

APPENDIX A

"CLEAN" VERSION OF EACH PARAGRAPH/SECTION/CLAIM
37 C.F.R. § 1.121(b)(ii) AND (c)(i)

SPECIFICATION:

Replacement for the paragraph beginning at page 3, line 28 to page 3, line 32:

However, even smart cards can be attacked, although in this case the attack must be sophisticated. This would imply the use of a virus or Trojan Horse to give commands to the card while it is activated without the user noticing anything unusual.

CLAIMS (with indication of amended or new):

1. (Amended) External signing device for a PC with an optical data input via the monitor, characterized in that said device includes an optical system for receiving the data from a computer monitor, an alphanumerical display for showing the data to be signed, a keyboard for user interaction with the device and a signing system to process the operations of signing the data received.

2. (Amended) Signing device as claimed in claim 1, characterized in that an area is defined in the monitor for transmitting data to the optical detector, in which area two sections have been defined, the first of which sends the data and the second sends a synchronization sequence used to distinguish inactive states from transmission of repeated bits, with the optical signal reception system further incorporating photo-detectors for detecting the signals sent from the sections in correspondence with the illumination changes of the display device.

3. (Amended) Signing device as claimed in claim 1 or 2, characterized in that it cannot be re-programmed, and in that it is activated by entering a personal identification number.

4. (Twice Amended) Signing device as claimed in claim 1 or claim 2, characterized in that it can show the signature on the display so that it can be copied to the destination device,

with said signature being generated by an encryption algorithm which uses the same key to sign and to verify said signature, so that the documents to be signed may contain any alphanumerical character and so that the data to be signed can be entered with a keyboard, and so that the user can view all messages in several languages.

5. (Twice Amended) Signing device as claimed in claim 1 or claim 2, characterized by the incorporation of an abbreviated signature generation algorithm of the symmetrical encryption type with the same key used to encode and decode, with the signature consisting of a subset of the bits generated by the encryption process, carrying out the signature verification process encrypting the data again and comparing the signature bits with the corresponding ones generated in the verification process, and with the signature encoded as 6-bit subsets so that it can be mapped onto a subset of printable ASCII characters.

7. (New) An external digital signing device, said device comprising:

a display, wherein said display displays output received from a computer;

an optical system, wherein said optical system receives said output from said display;

a keyboard, wherein said keyboard receives input from a user, and transmits said user input to said device; and

a signing system, wherein said signing system processes operations directed to digitally signing said output received from said display.

8. (New) The external digital signing device of claim 7, wherein said optical system further comprises photo-detectors, wherein said photo-detectors detect illumination changes in said display.

9. (New) The external digital signing device of claim 8, wherein said device defines at least a first section and a second section in said display, wherein said device further receives said output to be signed from said first section, and wherein said device further receives a

synchronization sequence to distinguish inactive states from transmission of repeated bits from said second section.

10. (New) The external digital signing device of claim 9, wherein said device is programmable and not re-programmable, and wherein said device is activated by entering a personal identification number.

11. (New) The external digital signing device of claim 9, wherein said display further displays a signature for said signing system, and wherein said signature is generated by an encryption algorithm.

12. (New) The external digital signing device of claim 11, wherein said encryption algorithm generates one key to sign said output and to verify said signature, and wherein said signed output includes at least one alphanumerical character.

13. (New) The external digital signing device of claim 9, wherein said device further incorporates an abbreviated signature generation algorithm for symmetrical encryption, wherein during verification of a signature, said output is re-signed and signature bits in said signed output are compared with signature bits in said re-signed output, and wherein said signature bits generated by said signing system are further compared with signature bits encoded as 6-bit subsets to be mapped onto a subset of printable ASCII characters.

14. (New) The external digital signing device of claim 9, wherein at least one of a plurality of languages is selectable for presenting said output to said user, and wherein one of a plurality of signature keys is selectable.

15. (New) The external digital signing device of claim 7, wherein said device programmable and not re-programmable, and wherein said device is activated by entering a personal identification number.

16. (New) The external digital signing device of claim 7, wherein said display further displays a signature for said signing system, and wherein said signature is generated by an encryption algorithm.

17. (New) The external digital signing device of claim 16, wherein said encryption algorithm generates one key to sign said output and to verify said signature, and wherein said signed output includes at least one alphanumerical character.

18. (New) The external digital signing device of claim 7, wherein said device further incorporates an abbreviated signature generation algorithm for symmetrical encryption, wherein during verification of a signature, said output is re-signed and signature bits in said signed output are compared with signature bits in said re-signed output, and wherein said signature bits generated by said signing system are further compared with signature bits encoded as 6-bit subsets to be mapped onto a subset of printable ASCII characters.

19. (New) The external digital signing device of claim 7, wherein at least one of a plurality of languages is selectable for presenting said output to said user, and wherein one of a plurality of signature keys is selectable.

APPENDIX B

VERSION WITH MARKINGS TO SHOW CHANGES MADE
37 C.F.R. § 1.121(b)(iii) AND (c)(ii)

SPECIFICATION:

Paragraph at page 3, line 28 to page 3, line 32:

However, even smart cards can be attacked, although in this case the attack must be sophisticated. This would imply the use of a virus or Trojan Horse to give commands to the card while it is activated without the [use] user noticing anything unusual.

CLAIMS:

1. (Amended) External signing device for a PC with an optical data input via the monitor, [immediately applicable to e-banking and e-commerce or to any other system based on electronic signatures which requires a high security with a relatively low quantity of data to be signed,] characterized in that said device includes an optical system [(1)] for receiving the data from a computer monitor [(2)], an alphanumerical display [(3)] for showing the data to be signed, a keyboard [(4)] for user interaction with the device and a signing system [meant] to process the operations of signing the data received.

2. (Amended) Signing device as claimed in claim 1, characterized in that an area [(6)] is defined in the monitor [(2)] for transmitting data to the optical detector [(1)], in which area two sections [(6, 6')] have been defined, the first of which sends the data and the second sends a synchronization sequence used to distinguish inactive states from transmission of repeated bits, with the optical signal reception system [(1)] further incorporating photo-detectors [(5)] for detecting the signals sent from the sections [(6')] in correspondence with the illumination changes of the display device.

3. (Amended) Signing device as claimed in claim 1 or 2, characterized in that it cannot be re-programmed, and in that it is activated by entering a personal identification number [(PIN)].

(Twice Amended) 4. Signing device as claimed in claim 1 or claim 2, characterized in that it can show the signature on the display [(3)] so that it can be copied to the destination device, with said signature being generated by an encryption algorithm which uses the same key to sign and to verify said signature, so that the documents to be signed may contain any alphanumerical character and so that the data to be signed can be entered with a keyboard, and so that the user can view all messages in several languages.

(Twice Amended) 5. Signing device as claimed in claim 1 or claim 2, characterized by the incorporation of an abbreviated signature generation algorithm of the symmetrical encryption type [(that is,] with the same key used to encode and decode[)], with the signature consisting of a subset of the bits generated by the encryption process, carrying out the signature verification process encrypting the data again and comparing the signature bits with the corresponding ones generated in the verification process, and with the signature encoded as 6-bit subsets so that it can be mapped onto a subset of printable ASCII characters.

P/4043-23

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

Fernando DE LA PUENTE ARRATE et al

Date: February 20, 2002

Serial No.:

Group Art Unit:

Filed:

Examiner:

For: EXTERNAL SIGNATURE DEVICE FOR A PC WITH OPTICAL DATA INPUT VIA THE MONITOR

U.S. Patent and Trademark Office
P.O. Box 2327
Arlington, VA 22202

Attn: Box PCT (US/DO/EO)

AMENDMENT/SUBMISSION

Prior to examination, please amend the application as follows.

FEE CALCULATION

Any additional fee required has been calculated as follows:

_____ If checked, "Small Entity" status is claimed.

	NO. CLAIMS AFTER AMENDMENT		HIGHEST NO. PREVIOUSLY PAID FOR		EXTRA PRESENT		RATE	ADDIT. FEE
TOTAL	10	MINUS	20	* =	0	X	($9 SE or $18)	$
INDEP.	1	MINUS	3	** =	0	X	($42 SE or $84)	$
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM						X	($140 SE or $280)	$ 280.00
* not less than 20 ** not less than 3							TOTAL	$ 280.00

If any additional payment is required, a check which includes the calculated fee of $280.00 (OFGS Check No. 8490) is attached.

In the event the actual fee is greater than the payment submitted or is inadvertently not enclosed or if any additional fee during the prosecution of this application is not paid, the Patent Office is authorized to charge the underpayment to Deposit Account No. 15-0700.

CONTINGENT EXTENSION REQUEST

If this communication is filed after the shortened statutory time period had elapsed and no separate Petition is enclosed, the Commissioner of Patents and Trademarks is petitioned, under 37 C.F.R. § 1.136(a), to extend the time for filing a response to the outstanding Office Action by the number of months which will avoid abandonment under 37 C.F.R. § 1.135. The fee under 37 C.F.R. § 1.17 should be charged to our Deposit Account No. 15-0700.

AMENDMENTS

_X_ If checked, amendment(s) to the specification and/or claims are submitted herewith.

1. ___ If checked, an abstract is submitted as the last page of Appendix A.

2. Claims:

Please amend claims 4-6 pursuant to 37 C.F.R. § 1.121(c)(i) as set forth in the "clean" version attached hereto as Appendix A. Entry is respectfully requested. A version with markings to show the changes made pursuant to 37 C.F.R. § 1.121(c)(ii) is attached hereto as Appendix B.

___ If checked, the optional complete set of "clean" claims pursuant to 37 C.F.R. § 1.121(c)(3) is attached hereto as Appendix C.

REMARKS/ARGUMENT

This Preliminary Amendment is being submitted to eliminate the improper multiple dependent claims.

EXPRESS MAIL CERTIFICATE

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail to Addressee (mail label # EL924372831US) in an envelope addressed to: U.S. Patent and Trademark Office, P.O. Box 2327, Arlington, VA 22202, on February 20, 2002:

Dorothy Jenkins
Name of Person Mailing Correspondence

Dorothy Jenkins
Signature

February 20, 2002
Date of Signature

Respectfully submitted,

James A. Finder
Registration No.: 30,173
OSTROLENK, FABER, GERB & SOFFEN, LLP
1180 Avenue of the Americas
New York, New York 10036-8403
Telephone: (212) 382-0700

EL924372831US

APPENDIX A

"CLEAN" VERSION OF EACH PARAGRAPH/SECTION/CLAIM
37 C.F.R. § 1.121(b)(ii) AND (c)(i)

CLAIMS (with indication of amended or new):

(Amended) 4. Signing device as claimed in claim 1 or claim 2, characterized in that it can show the signature on the display (3) so that it can be copied to the destination device, with said signature being generated by an encryption algorithm which uses the same key to sign and to verify said signature, so that the documents to be signed may contain any alphanumerical character and so that the data to be signed can be entered with a keyboard, and so that the user can view all messages in several languages.

(Amended) 5. Signing device as claimed in claim 1 or claim 2, characterized by the incorporation of an abbreviated signature generation algorithm of the symmetrical encryption type (that is, with the same key used to encode and decode), with the signature consisting of a subset of the bits generated by the encryption process, carrying out the signature verification process encrypting the data again and comparing the signature bits with the corresponding ones generated in the verification process, and with the signature encoded as 6-bit subsets so that it can be mapped onto a subset of printable ASCII characters.

(Amended) 6. Signing device as claimed in claim 1 or claim 2, characterized in that one of several currencies can be chosen for the monetary amounts of the documents to be signed, one of several signature keys can be chosen and one of several languages can be chosen for presenting the messages to the user.

APPENDIX B

VERSION WITH MARKINGS TO SHOW CHANGES MADE
37 C.F.R. § 1.121(b)(iii) AND (c)(ii)

CLAIMS:

4. Signing device as claimed in [one or more of the previous claims 1 to 3] claim 1 or claim 2, characterized in that it can show the signature on the display (3) so that it can be copied to the destination device, with said signature being generated by an encryption algorithm which uses the same key to sign and to verify said signature, so that the documents to be signed may contain any alphanumerical character and so that the data to be signed can be entered with a keyboard, and so that the user can view all messages in several languages.

5. Signing device as claimed in [one or more of the previous claims] claim 1 or claim 2, characterized by the incorporation of an abbreviated signature generation algorithm of the symmetrical encryption type (that is, with the same key used to encode and decode), with the signature consisting of a subset of the bits generated by the encryption process, carrying out the signature verification process encrypting the data again and comparing the signature bits with the corresponding ones generated in the verification process, and with the signature encoded as 6-bit subsets so that it can be mapped onto a subset of printable ASCII characters.

6. Signing device as claimed in [one or more of the previous claims] claim 1 or claim 2, characterized in that one of several currencies can be chosen for the monetary amounts of the documents to be signed, one of several signature keys can be chosen and one of several languages can be chosen for presenting the messages to the user.